



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/881,899	06/14/2001	Chee-Hong Wong	23615-05503	8876

21919 7590 09/21/2006

MEREK, BLACKMON & VOORHEES, LLC  
673 S. WASHINGTON ST.  
ALEXANDRIA, VA 22314

EXAMINER

SON, LINH L D

ART UNIT PAPER NUMBER

2135

DATE MAILED: 09/21/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/881,899

Applicant(s)

WONG ET AL.

Examiner

Linh LD Son

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 30 June 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-26 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1,5-11,13-18 and 22-26 is/are rejected.
- 7) ☒ Claim(s) 2-4,12 and 19-21 is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                       | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

### **DETAILED ACTION**

1. This Office Action is responding to the Amendment received on 06/30/06.
2. Claims 1-26 are pending.

### ***Response to Arguments***

3. Applicant's arguments filed June 30<sup>th</sup>, 2006 have been fully considered but they are not persuasive.
4. As per remark on page 2, applicant argues that Smith does not teach "sending to the addressee a notification of the delivery; and in response to receiving an acknowledgement from the addressee: obtaining a new public key of the addressee; decrypting the package decryption key". As per rejection on 12/30/05, Smith discloses the notification of the delivery and response to the notification of the delivery by sending the public key to the server for use to encrypt the encryption key (Smith, Col 5 lines 10-20), and Smith's teaching was incorporate with Dorenbos. Dorenbos on the other hand discloses the "obtaining a new public key of the addressee (Fig 4 # 409, Col 4 lines 55-60); decrypting package decryption key (Col 3 lines 26-30); encrypting the package decryption key with the addressee's new public key (Col 3 lines 32-36, and Col 4 lines 55-60); and transmitting to the addressee the information package encrypted with the package encryption key and the package decryption key encrypted with the addressee's new public key (Col 3 lines 32-38).

Art Unit: 2135

5. As per remark on page 2 2<sup>nd</sup> paragraph, Applicant argues, that "an escrow key is first applied to the document" is not taught in Smith. Again, Derenbos discloses the "escrow key" as the server public key (Fig 2, #105). Further Applicant argues that Smith does not teach "the escrow key is removed prior to applying the new recipient key which refers to the limitation "decrypting the package decryption key; encrypting the package decryption key with the addressee's new public key"". This limitation again is taught in Derenbos in

(Col 3 lines 26-38)

The encryption server 101 decrypts the second-stage encrypted message 105 using an appropriate key. In the preferred embodiment, the appropriate key is the encryption server's private key. The encryption server 101 then determines the user's ID from the decrypted message and also determines the IDs of all recipients that the user indicated as intended targets of the first-stage encrypted message. The encryption server 101 then encrypts the user's ID along with the first-stage encrypted message by encrypting with the public key of the first recipient.

In Col 4 lines 40-67:

As shown in FIG. 2, a user message 105 comprises a second-stage encrypted (encrypted using the encryption server's public key) message comprising the digital data message 105A, first-stage encrypted with the user's (sender's) private key, in addition to the user ID and a number of recipient IDs. Alternatively, the user message 105 may comprise an unencrypted digital data message 105A, the user ID, and one or more recipient IDs. The user message 105 is input to the receive wireline/wireless block 207, the output of which is input to the processor(s) 201. The processor(s) 201 utilize(s) the encryption/decryption algorithm(s) 203 and the public key data base 205 to decrypt the message 105 using the private key of the encryption server. The processor(s) 201 then determine(s) the first-stage encrypted message 105A, the user ID, and the first recipient ID from the decrypted message. The processor(s) 201 then determine(s) the first recipient's public key from public key data base 205, and the encrypt the first-stage encrypted message 105A and the user ID by using the encryption/decryption algorithms 203 and the first recipient's public key. The processor(s) 201 then append(s) the first recipient ID, thereby yielding a message 109 that is sent to the transmit wireline/wireless block 209 for transmitting to the first recipient's communication unit 111, as shown in FIG. 1. A similar process is performed on the first-stage encrypted message (or unencrypted digital data message) 105A and the user ID for each of the recipients listed in the user's message 105.

Art Unit: 2135

Then, The applicant presumes that the Examiner interpreted the new recipient's key and the escrow key were the same. As recited above, it is clearly that the new recipient's key and the escrow key are not the same.

6. Same rejection basis is applicable to claim 11 and 18.

7. As per argument regarding to claim 1, 11, and 18, Applicant made argument based on the secondary art, "Smith". Examiner rejected these claims based on the primary reference, Dorenbos, and secondary reference, Smith. Examiner respectfully cannot rebut the Applicant's argument based on only the secondary reference, Smith, wherein the primary reference, Dorenbos, were used to reject the claim limitations. See the Office Action dated 12/30/05.

8. Applicant's arguments, see Amendment, filed 06/30/06, with respect to claims 2, 12, and 19 have been fully considered and are persuasive. The rejection basis of claims 2, 12, and 19 in the Office Action dated 12/30/05 has been withdrawn.

### ***Claim Rejections - 35 USC § 103***

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Art Unit: 2135

10. Claims 1, 5-11, 13-18, and 22-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dorenbos, US Patent No. 5751813, in view of Smith et al, US Patent No. 6061448, hereinafter "Smith".

11. As per claim 1:

Dorenbos teaches "A computer-implemented method for securely transmitting an information package from a sender to an addressee via a network (Fig. 1), the method comprising a server system performing the steps of: receiving a delivery from the sender, the delivery comprising: the information package encrypted with a package encryption key (Fig 2, User Private key); and a package decryption key (User ID) encrypted with an escrow key (Fig 2, #105, Encryption Server Public key); storing the delivery in escrow for the addressee; sending to the addressee a notification of the delivery; and in response to receiving an acknowledgement from the addressee: obtaining a new public key of the addressee (Fig 4 # 409, Col 4 lines 55-60); decrypting the package decryption key (Col 3 lines 26-30); encrypting the package decryption key with the addressee's new public key (Col 3 lines 32-36, and Col 4 lines 55-60); and transmitting to the addressee the information package encrypted with the package encryption key and the package decryption key encrypted with the addressee's new public key (Col 3 lines 32-38).

However, Dorenbos does not directly teach of the decryption key.

Nevertheless, Dorenbos teaches of encrypting the User ID of the sender with the package and the receiver or addressee uses the User ID to obtain the correct decryption key to decrypt the message. Therefore, it would have been obvious at the

Art Unit: 2135

time of the invention was made for one ordinary skill in the art to modify Dorenbos invention to include the encryption key with the delivery so that the user does not need to store the sender key to decrypt the message.

Further, Dorenbos does not teach of storing the delivery in escrow for the addressee; sending to the addressee a notification of the delivery; and in response to receiving an acknowledgement from the addressee:

Nevertheless, Smith discloses a "Method and System for Dynamic Server Document Encryption" invention, which including a server computer sends, receives, and stores secure data provided by authorized users. Server computer receives the encrypted document from user, stores it securely, and sends notification to the recipient. In response to the recipient response, the server sends the delivery to the recipient (Col 5 lines 5-30).

Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify Dorenbos's invention to incorporate Smith's storage and notification feature to make sure that the user is ready to receive the delivery.

12. As per claims 11, and 18:

Dorenbos teaches "A system, a method and an apparatus for securely transmitting an information package from a sender to an addressee via a network (Fig. 1), the system comprising: a storage module, comprising a computer-readable storage medium, for receiving, and storing in escrow, a delivery from the sender, said delivery comprising: a package decryption key (User ID) encrypted with an escrow key, and the information

Art Unit: 2135

package encrypted with a package encryption key (Fig 2, #105, Encryption Server Public key); a notification module coupled to the storage module, for sending a notification to the addressee via the network; a key registration module coupled to the notification module for, in response to receiving an acknowledgement from the addressee, receiving a new public key of the addressee; and a transmission module coupled to the storage module, for decrypting the package decryption key and re-encrypting the package decryption key with the new public key of the addressee (Col 3 lines 32-36, and Col 4 lines 55-60), and for transmitting to the addressee the information package encrypted with the package encryption key and the package decryption key encrypted with the addressee's new public key (Col 3 lines 32-38).

However, Dorenbos does not directly teach of the decryption key.

Nevertheless, Dorenbos teaches of encrypting the User ID of the sender with the delivery and the receiver or addressee uses the User ID to obtain the correct decryption key to decrypt the message. Therefore, it would have been obvious at the time of the invention was made for one ordinary skill in the art to modify Dorenbos invention to include the encryption key with the delivery so that the user does not need to store the sender key to decrypt the message.

Further, Dorenbos does not teach of a notification module coupled to the storage module, for sending a notification to the addressee via the network; a key registration module coupled to the notification module for, in response to receiving an acknowledgement from the addressee, receiving a new public key of the addressee.



Nevertheless, Smith discloses a "Method and System for Dynamic Server Document Encryption" invention, which including a server computer sends, receives, and stores secure data provided by authorized users. Server computer receives the encrypted document from user, stores it securely, and sends notification to the recipient. In response to the recipient response, the server sends the delivery to the recipient (Col 5 lines 5-30). Further, Smith also teaches of a key registration module to receive a new public key of the recipient or addressee (Col 5 lines 9-19).

Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify Dorenbos's invention to incorporate Smith's storage and notification feature to make sure that the user is ready to receive the delivery.

13. As per claims 5, 13-14, and 22:

Dorenbos and Smith teach "The method of claims 1, 11, and 18". Further Smith discloses "the server system performing the steps of: registering and issuing the new public key to the addressee; and storing the addressee's new public key in a public key database" in (Col 5 lines 1-15).

14. As per claims 6 and 15:

Dorenbos and Smith teach "The method of claims 1 and 11". Wherein Smith discloses "the escrow key is one of a group comprising a symmetric key and an asymmetric key" in (Col 4 lines 8, asymmetric key equals to public/private key).

Art Unit: 2135

15. As per claims 7, 16, and 23:

Dorenbos and Smith teach "The method of claims 1, 11, and 18". Wherein Smith discloses "the notification is one of a group comprising an e-mail notification, a desktop notification, a voice notification, a pager notification, and a facsimile notification" in (Col 5 lines 1-15).

16. As per claims 8 and 24:

Dorenbos and Smith teach "The method of claims 1 and 18". Further Smith discloses "the server system performing the steps of: receiving from the sender a digest of one from a group comprising: the information package; the information package encrypted with the package encryption key; and the information package encrypted with the package encryption key and the package decryption key encrypted with the escrow key; and in response to receiving the acknowledgement from the addressee: transmitting the digest to the addressee" in (Col 5 lines 1-30, and Col 6 lines 40-67).

17. As per claims 9, 25:

Dorenbos and Smith teach "The method of claims 8 and 25". Wherein Smith discloses "the digest is encrypted by a private key of the sender" in (Col 3 lines 1-6).

18. As per claims 10, 17, and 26:

Dorenbos and Smith teach "The computer-readable medium of claims 1, 11, and 18". Further Smith discloses "program code adapted to perform the step of: authenticating the addressee prior to transmitting the information package encrypted with the package

Art Unit: 2135

encryption key and the package encryption key encrypted with the addressee's new public key" in (Col 5 lines 1-53) and the rejection of claim is incorporated.

***Allowable Subject Matter***

19. Claims 2-4, 12, and 19-21 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

***Conclusion***

20. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

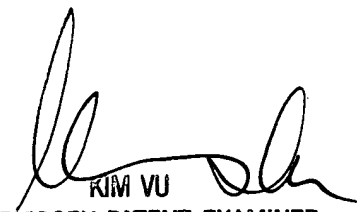
Art Unit: 2135

21. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Linh LD Son whose telephone number is 571-272-3856. The examiner can normally be reached on 9-6 (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Linh LD Son  
Examiner  
Art Unit 2135

  
KIM VU  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100